

*U.S. Patent Application Serial No. 10/003,819**Attorney Docket No. 10017333-1***REMARKS**

This Application has been carefully reviewed in light of the Office Action mailed August 26, 2006. Applicants have amended Claims 13 and 15; Claims 1-15 remain pending. Upon entry of this paper, Applicants respectfully request consideration and allowance of all claims.

Claims 1-5 and 13-15 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*"). Of the rejected claims, Claim 1 is independent. Applicants respectfully submit that independent Claims 1 and 13 are patentable over *Vaidya* and, therefore, Claims 1 and 13, together with Claims 2-5 and 14-15 that depend respectively therefrom, are in condition for allowance.

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claims” and “[t]he elements must be arranged as required by the claim.” *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

Independent Claim 1 recites, at least in part, “a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver and bound to the protocol driver and the media access control driver” (emphasis added). In the Final Office Action, the Examiner refers generally to column 6, lines 11-18, column 7, lines 12-24, and figure 2 of *Vaidya* as disclosing the above-references limitation(s) (Final Office Action, pages 3 and 4). However, Applicants respectfully submit that the above-referenced limitation(s) are not disclosed or even suggested in the portions of *Vaidya* referred to by the Examiner or elsewhere in *Vaidya*. For example, *Vaidya* does not appear to disclose or even suggest a network stack as recited by independent Claim 1 having a protocol driver, a media access

control driver and “an instance of [an] intrusion prevention system implemented as an intermediate driver” as recited by Claim 1. Thus, the Examiner has not established a *prima facie* case of anticipation of independent Claim 1 at least because *Vaidya* does not disclose or even suggest “[t]he identical invention . . . in as complete detail as is contained in . . . the claim,” nor has the Examiner provided any of the required reasoning or bases to support the rejection of Claim 1 pursuant to the courts and the M.P.E.P. Therefore, Applicants respectfully submit the rejection of Claims 1 is improper and should be withdrawn.

Additionally, in response to Applicants’ arguments in a response filed June 10, 2005, the Examiner refers to column 4, lines 28-33, of *Vaidya* which recites:

An advantage of the present invention is that all seven layers of the OSI model are monitored and so an attack based in any of the layers can be detected.

(*Vaidya*, column 4, lines 28-31). *Vaidya* also recites:

The virtual processor 36 obtains a data packet from a queue and extracts MAC header information, IP header information, transport header information, and application information from the data packet.

(*Vaidya*, column 7, lines 18-21). Thus, the monitoring of the seven layers of the OSI model of *Vaidya* referred to by the Examiner appears to be limited to pulling a data packet from a queue and then extracting data from the data packet for analysis. Instead, Applicants’ Claim 1 recites that intrusion protection is implemented as part of “a network stack [of an operating system]” and, specifically, implemented as “an intermediate driver” of the network stack. Accordingly, Applicants respectfully submit that for at least this reason also, *Vaidya* does not anticipate Claim 1.

Therefore, Applicants respectfully submit that independent Claim 1 is patentable over the *Vaidya* reference. Thus, Claim 1 and respective dependent Claims 2-5 are in condition for allowance.

*U.S. Patent Application Serial No. 10/003,819**Attorney Docket No. 10017333-1*

Claims 13-15 are rejected under 35 U.S.C. §102(e) as being anticipated by *Vaidya*. Of the rejected claims, Claim 13 is independent. Applicants respectfully submit that independent Claim 13 is patentable over *Vaidya* and, therefore, independent Claim 13 and respective dependent Claims 14 and 15 are in condition for allowance.

Amended independent Claim 13 recites, at least in part, “determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures” (emphasis added). Regarding Claim 13, the Examiner refers to column 6, line 57, through column 7, line 10, of *Vaidya* as disclosing the limitations of independent Claim 13 (Final Office Action, pages 2, 3 and 5). Applicants respectfully disagree. In the Final Office Action, the Examiner admits that *Vaidya* does not explicitly show determining correspondence between the packet and at least two of the network-exploit signatures (Final Office Action, page 7). For at least this reason, Claim 13 is not anticipated by *Vaidya*. Therefore, Applicants respectfully submit that Claim 13 is patentable over the *Vaidya* reference. Claim 15 has been amended on a strictly antecedent basis to track the amended phrasing of independent claim 13. Thus, Claim 13 and respective dependent Claims 14 and 15 are in condition for allowance.

Claims 6-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Vaidya* in view of U.S. Patent No. 6,578,147 issued to Shanklin et al. (hereinafter “*Shanklin*”). Of the rejected claims, Claim 6 is independent. Applicants respectfully submit that neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 6. Therefore, Applicants respectfully submit that Claim 6, and Claims 7-12 that depend therefrom, are in condition for allowance.

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references

*U.S. Patent Application Serial No. 10/003,819**Attorney Docket No. 10017333-1*

when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishaw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

Independent Claim 6 recites "comparing the packet with a plurality of machine-readable network-exploit signatures" and "determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures" (emphasis added). In the Final Office Action, the Examiner admits that *Vaidya* does not explicitly show determining correspondence between the packet and at least two of the network-exploit signatures (Final Office Action, page 7). However, the Examiner states that *Shanklin* discloses an intrusion detection system that forwards packets from different sessions to a network analyzer to be used in detecting certain types of composite signatures, and that it would have been obvious to modify *Vaidya* with the teaching of *Shanklin* to arrive at Applicants' Claim 6 (Final Office Action, page 7). Applicants respectfully disagree.

The portion of *Shanklin* referred to by the Examiner in the Office Action states:

A network analyzer 25 receives packets from different sessions, which may be used to detect certain types of composite signatures. For example, a "ping" type signature

is indicated by multiple sessions that attempt to connect to different destinations with the local network. Single packets indicating ping behavior can be delivered to network analyzer 25, which then monitors similar packets from different sessions to see if a ping pattern is indicated. In general, network analyzer 25 detects signatures of attacks against multiple hosts and different sessions. Such attacks are often detected using statistical correlations.

(*Shanklin*, column 5, lines 29-39). Applicants respectfully submit that monitoring packets from different sessions is not equivalent to "determining a correspondence between [a] packet and at least two of the plurality of machine-readable network-exploit signatures" as recited by Claim 6 (emphasis added) which is clearly not disclosed or even suggested by the portion of *Shanklin* referred to by the Examiner or elsewhere in *Shanklin*. Further, as apparently recognized by the Examiner, *Vaidya* does not remedy at least this deficiency of *Shanklin*. Accordingly, Applicants respectfully submit that neither *Vaidya* nor *Shanklin*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 6.

Therefore, Applicants respectfully submit that Claim 6 is patentable over the cited references. Thus, Claim 6 and respective dependent Claims 7-12 are in condition for allowance.

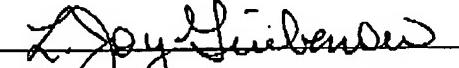
CONCLUSION

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request consideration and full allowance of all pending claims.

Other than the fee for filing of an RCE (see accompanying Request for Continuing Examination paperwork), no additional fee is believed due as a result of this Preliminary Amendment. If, however, Applicants have overlooked the need for any fee due as a result of this Preliminary Amendment, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Preliminary Amendment to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

Date: January 23, 2006


L.Joy Griebeinow
Reg. No. 33,704
Attorney for Applicants

Correspondence to:
L.Joy Griebeinow, Esq.
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400
(970) 898-3884